

1 QUINN EMANUEL URQUHART & SULLIVAN, LLP

2 Andrew H. Schapiro (*Pro Hac Vice*)
3 *andrewschapiro@quinnemanuel.com*
4 191 N. Wacker Drive, Suite 2700
5 Chicago, IL 60606-1881
6 Telephone: (312) 705-7400

7 David Eiseman (Bar No. 114758)
8 *davideiseman@quinnemanuel.com*
9 50 California Street, 22nd Floor
10 San Francisco, California 94111-4788
11 Telephone: 415-875-6600
12 Fax: 415-875-6700

13 Stefan Berthelsen (*Pro Hac Vice*)
14 *stefanberthelsen@quinnemanuel.com*
15 51 Madison Ave 22nd floor
16 New York, NY 10010
17 Telephone: (212) 849-7014

18 *Attorneys for Plaintiff*
19 *X Corp.*

20
21
22
23
24
25
26
27
28
UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

X CORP., a Nevada corporation,

Plaintiff,

vs.

BRIGHT DATA LTD., an Israeli
corporation,

Defendant.

Case No. 3:23-cv-03698-WHA

**PLAINTIFF'S NOTICE OF MOTION AND
MOTION FOR LEAVE TO AMEND
COMPLAINT; SUPPORTING
MEMORANDUM OF POINTS AND
AUTHORITIES**

Date: July 25, 2024

Time: 8:00 a.m.

REDACTED FOR PUBLIC FILING

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE THAT on July 25, 2024 at 8:00 a.m. or as soon thereafter as the matter may be heard before the Honorable William H. Alsup, United States District Judge for the Northern District of California, Plaintiff X Corp. (“X”) will, and hereby does, move this Court, pursuant to Rule 15(a)(2) of the Federal Rules of Civil Procedure for leave to amend its Complaint.

This Motion is based on this Notice of Motion and Motion, the Memorandum of Points and Authorities set forth below, the accompanying Declaration of Andrew H. Schapiro, the other documents on file in this action, and any oral argument of counsel at the hearing on the Motion.

DATED: June 6, 2024

Respectfully submitted,

QUINN EMANUEL URQUHART &
SULLIVAN, LLP

By /s/ Andrew H. Schapiro

Andrew H. Schapiro
David Eiseman
Stefan Berthelsen

Attorneys for Plaintiff X Corp.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

Page

I.	INTRODUCTION.....	1
II.	BACKGROUND.....	1
III.	LEGAL STANDARD.....	2
IV.	ARGUMENT	3
A.	X's Amendments Are Not Futile And Would Survive A Motion To Dismiss	3
1.	Damage Flowing From Bright Data's Access of X's Servers.....	3
(a)	<i>Trespass to Chattels</i>	4
(b)	<i>Tortious Interference with Contract</i>	5
(c)	<i>Breach of Contract</i>	6
2.	Amended Data Scraping Claims Are Not Preempted	6
(a)	<i>Preventing Bright Data's Scraping Will Protect X Users' Privacy</i>	7
(b)	<i>Election Integrity and Public Conversation Manipulation</i>	9
(c)	<i>X and Consumer Protection</i>	10
(d)	<i>Regulating Economic Activity</i>	11
3.	Misappropriation of X's Aggregated Data At Scale	12
B.	X's Amendments Are Timely And Do Not Prejudice Bright Data	14
V.	CONCLUSION	15

TABLE OF AUTHORITIES**Page****Cases**

<i>Andrews v. Daughtry</i> , No. 12-cv-00441, 2013 WL 664564 (M.D.N.C. Feb. 22, 2013)	11
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	2
<i>Barclays Capital Inc. v. Theflyonthewall.com, Inc.</i> , 650 F.3d 876 (2d Cir. 2011)	12
<i>Bates v. Dow Agrosciences LLC</i> , 544 U.S. 431 (2005)	9
<i>Bell Atl. Corp. V. Twombly</i> , 550 U.S. 544 (2007)	2
<i>Bonito Boats, Inc. v. Thunder Craft Boats, Inc.</i> , 489 U.S. 141 (1989)	6
<i>Civic Western Corp v. Zila Industries, Inc.</i> , 135 Cal. Rptr. 915 (Cal. Ct. App. 1977)	5
<i>Cnty. of San Bernardino v. Walsh</i> , 69 Cal. Rptr. 3d 848 (Cal. Ct. App. 2007)	11
<i>Compulife Software Inc. v. Newman</i> , 959 F.3d 1288 (11th Cir. 2020)	13
<i>DCD Programs, Ltd. V. Leighton</i> , 833 F.2d 183 (9th Cir. 1987)	2
<i>Digital Drilling Data Systems, LLC v. Petrolink Services, Inc.</i> , 965 F.3d 365 (5th Cir. 2020)	11
<i>eBay, Inc. v. Bidder's Edge, Inc.</i> , 100 F. Supp. 2d 1058 (N.D. Cal. 2000)	5
<i>Eminence Cap., LLC v. Aspeon, Inc.</i> , 316 F.3d 1048 (9th Cir. 2003)	2, 14, 15
<i>Facebook, Inc. v. ConnectU LLC</i> , 489 F. Supp. 2d 1087 (N.D. Cal. 2007)	14
<i>Facenda v. N.F.L. Films, Inc.</i> , 542 F.3d 1007 (3d Cir. 2008)	7

1	<i>Garcia v. Google, Inc.</i> ,	
2	786 F.3d 733 (9th Cir. 2015)	6
3	<i>General Motor Corps v. Abrams</i> ,	
4	897 F.2d 34 (2d Cir. 1990).....	9
5	<i>Goldstein v. California</i> ,	
6	412 U.S. 546 (1973)	11
7	<i>Gonzalez v. Google LLC</i> ,	
8	2 F.4th 871 (9th Cir. 2021), rev'd sub nom. on other grounds,	
9	<i>Twitter, Inc. v. Taamneh</i> , 598 U.S. 471 (2023)	9
10	<i>Hollywood Screentest of Am., Inc. v. NBC Universal, Inc.</i> ,	
11	151 Cal. App. 4th 631 (2007)	12
12	<i>I-CA Enterprises, Inc. v. Palram Americas, Inc.</i> ,	
13	185 Cal. Rptr. 3d 24 (Cal. App. Ct. 2015)	11
14	<i>Int'l News Serv. v. Associated Press</i> ,	
15	248 U.S. 215 (1918)	12
16	<i>Intel Corp. v. Hamidi</i> ,	
17	71 P.3d 296 (Cal. 2003)	4
18	<i>In re Jackson</i> ,	
19	972 F.3d 25 (2d. Cir. 2020)	6, 9
20	<i>Johnson v. Serenity Transportation, Inc.</i> ,	
21	No. 15-cv-02004-JSC, 2015 WL 4913266 (N.D. Cal. Aug. 17, 2015).....	14
22	<i>In re JUUL Labs, Inc., Mktg., Sales Pracs., & Prod. Liab. Litig.</i> ,	
23	497 F. Supp. 3d 552 (N.D. Cal. 2020)	9
24	<i>Knight v. Jewett</i> ,	
25	834 P.2d 696 (Cal. 1992)	4, 5
26	<i>Nat'l Basketball Ass'n v. Motorola, Inc.</i> ,	
27	105 F.3d 841 (2d Cir. 1997)	12
28	<i>Oasis W. Realty, LLC v. Goldman</i> ,	
	250 P.3d 1115 (Cal. 2011)	6
	<i>Ohio v. Am. Express Co.</i> ,	
	585 U.S. 529 (2018)	14
	<i>Pac. Gas & Elec. Co.v. Bear Stearns & Co.</i> ,	
	791 P.2d 587 (Cal. 1990)	5

1	<i>People.ai, Inc. v. Clari Inc.</i> ,	
2	No. 21-cv-06314 WHA, 2022 WL 228306 (N.D. Cal. Jan. 26, 2022)	2
3	<i>Shelton v. Comercia Bank</i> ,	
4	No. 23-cv-02815 (WHA), 2024 WL 234721 (N.D. Cal. Jan. 22, 2024) (Alsup, J.)	2
5	<i>Sonos Inc. v. Google LLC</i> ,	
6	No. 21-cv-7559 (WHA), 2022 WL 2046828 (N.D. Cal. June 7, 2022).....	2
7	<i>Stackla, Inc. v. Facebook Inc.</i> ,	
8	No. 19-cv-05849 PJH, 2019 WL 4738288 (N.D. Cal. Sept. 27, 2019)	8
9	<i>Wyeth v. Levine</i> ,	
10	555 U.S. 555 (2009)	6

Rules

11	Fed. R. Civ. P. 15(a)(2)	2
----	--------------------------------	---

Statutes

12	California Business and Professions Code Section 17200.....	3
----	---	---

Other Authorities

13	<i>Fight AI-Backed Voter Suppression</i> , BRENNAN CTR. FOR JUSTICE (Apr. 16, 2024),	
14	available at https://www.brennancenter.org/our-work/research-reports/preparing-	
15	fight-ai-backed-voter-suppression	10
16	Glob. Priv. Assembly, Int’l Enft Coop. Working Grp.,	
17	<i>Joint Statement on Data Scraping and the Protection of Privacy</i> (Aug. 24, 2023),	
18	https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-	
19	scraping-202308.pdf	8
20	Note, Geoffrey Xiao, <i>Bad Bots: Regulating the Scraping of Public Personal</i>	
21	<i>Information</i> , 34 HARV. J. L. & TECH. 702, 711 (2021)	8
22	Orin S. Kerr, <i>The Mosaic Theory of the Fourth Amendment</i> , 111 MICH. L. REV. 311	
23	(2012)	12

1 **I. INTRODUCTION**

2 This Court dismissed X’s First Amended Complaint (“FAC”), citing two primary categories
3 of deficiencies: insufficient allegations of harm, and insufficient allegations of independent state
4 interests that would preclude preemption by the Copyright Act. In so ruling, the Court invited X to
5 seek to cure those perceived failings, which X now does with its proposed Second Amended
6 Complaint (“SAC”). The SAC alleges significant, quantifiable harms flowing from Bright Data’s
7 and its customers’ conduct. It also avers facts demonstrating that its claims implicate not only
8 copyright concerns, but other significant state interests, including user privacy, consumer protection,
9 election integrity, and the regulation of economic activity. The SAC accordingly should survive a
10 Bright Data motion to dismiss, and amendment would not be futile. No other factor under Rule
11 15(a)(2)’s liberal standard—prejudice to Bright Data, undue delay, repeated failure to cure
12 deficiencies, or bad faith—is applicable. This Court should therefore grant X leave to amend.

13 **II. BACKGROUND**

14 X brought this action against Bright Data, alleging breach of contract, tortious interference
15 with contract, and unjust enrichment. ECF No. 1. X amended its complaint once as a matter of
16 course and added trespass to chattels, California business fraud, and misappropriation claims. ECF
17 No. 36. After initial and supplemental briefing, ECF Nos. 42, 48, 49, 60, 61, 63, 64, the Court
18 dismissed X’s claims, structuring its analysis in two general categories (with some overlap): first,
19 claims based on Bright Data’s accessing of X’s platform and servers, and second, claims based on
20 Bright Data’s scraping and selling of X’s data. *See* ECF No. 83 (“Op.”). First, the Court found
21 conclusory X’s allegations that Bright Data’s access of X’s platform and servers resulted in
22 cognizable harm to X in any quantifiable way. *Id.* Second, the Court found X’s claims premised on
23 Bright Data’s scraping and sale of X’s platform to be impliedly preempted, without any allegations
24 to support a substantial state interest that could resuscitate them. *Id.*

25 The Court provided that “X Corp. may seek leave to amend its complaint by motion no later than
26 **THURSDAY, JUNE 6, AT NOON.** Any motion for leave to amend should affirmatively demonstrate how
27 the proposed amended complaint corrects deficiencies identified in this order as well as all other
28 deficiencies raised in Bright Data’s motion. It should be accompanied by a redlined copy of the proposed

1 amended complaint showing all proposed amendments.” Op. at 26 (emphasis in original). X now so
 2 moves with a clean proposed SAC, a redlined copy of the same, and a proposed order attached. Exh. A-
 3 C.

4 **III. LEGAL STANDARD**

5 Federal courts are directed to “freely give leave” to amend pleadings “when justice so
 6 requires.” Fed. R. Civ. P. 15(a)(2). This policy is “to be applied with extreme liberality.” *Eminence*
 7 *Cap., LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1051 (9th Cir. 2003) (reversing denial of leave to amend).
 8 “When determining whether to grant leave, a district court considers: (1) bad faith; (2) undue delay;
 9 (3) prejudice to the opposing party; (4) futility of amendment; and (5) repeated failure to cure
 10 deficiencies despite previous amendments. Prejudice to the opposing party is the touchstone of the
 11 inquiry under rule 15(a), and carries the greatest weight.” *Shelton v. Comercia Bank*, No. 23-cv-
 12 02815 (WHA), 2024 WL 234721, at *2 (N.D. Cal. Jan. 22, 2024) (Alsup, J.) (internal quotation marks
 13 and citations omitted) (quoting *Eminence*, 316 F.3d at 1052). In the absence of futility, undue delay,
 14 or prejudice to the defendant, there is a “*presumption* under Rule 15(a) in favor of granting leave to
 15 amend.” *Eminence*, 316 F.3d at 1052 (emphasis in original).

16 An amended complaint properly states a claim “when the factual allegations permit a
 17 reasonable inference, not just speculation, that the defendant is liable for the misconduct alleged.”
 18 *People.ai*, 2022 WL 228306, at *2. “All factual allegations rate as true, but legal conclusions
 19 merely couched as fact may be disregarded.” *Id.* (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678
 20 (2009); *Bell Atl. Corp. V. Twombly*, 550 U.S. 544, 555 (2007); *DCD Programs, Ltd. V. Leighton*,
 21 833 F.2d 183, 186 (9th Cir. 1987)). And “[a] motion to make an amendment is to be liberally
 22 granted where from the underlying facts or circumstances, the plaintiff may be able to state a
 23 claim.” *Sonos Inc. v. Google LLC*, No. 21-cv-7559 (WHA), 2022 WL 2046828, at *2 (N.D. Cal.
 24 June 7, 2022) (internal quotation marks omitted) (quoting *DCD Programs, Ltd. v. Leighton*, 833
 25 F.2d 183, 186 (9th Cir. 1987)).

IV. ARGUMENT

The SAC plausibly alleges that Bright Data's access of X's servers caused cognizable harm to X and that Bright Data's scraping and selling of X and its users' data implicates important state interests beyond copyright, and therefore is not preempted.

A. X's Amendments Are Not Futile And Would Survive A Motion To Dismiss

1. Damage Flowing From Bright Data's Access of X's Servers¹

The Court dismissed X's trespass to chattels, tortious interference with contract, and breach of contract claims for want of adequate allegations of injury. *Op.* at 9-11, 14-17. The SAC now quantifies the severely diminished server capacity flowing from Bright Data's and its customers breach of X's Terms. While X's [REDACTED] is designed to ensure that its system overall is less likely to fail entirely, [REDACTED] hosting [REDACTED] are more [REDACTED]: [REDACTED] of attempts to view an [REDACTED] are anomalous or inauthentic; [REDACTED] of the web requests to look up a [REDACTED] are anomalous or inauthentic; [REDACTED] of the web requests to look up a [REDACTED] are anomalous or inauthentic; [REDACTED] of requests to look up a [REDACTED] are inauthentic; [REDACTED] of web requests to access a particular user's follower graph are inauthentic; and [REDACTED] of [REDACTED] are anomalous or inauthentic. ¶¶ 68-72.² These [REDACTED] are almost certainly the result of automated scraping because the [REDACTED]—indeed, Bright Data advertises scraping some of them. *See* ¶¶ 76-82. In sum total, on average [REDACTED]. ¶ 70. Beyond the server costs themselves, X incurs additional ongoing operational and maintenance costs related to the team of engineers it must employ to play whack-a-mole as the automated, anomalous access tactics of scrapers like Bright Data evolve. ¶ 73.

¹ Mindful of the deficiencies which the Court identified, *Op.* at 11-13, X repleads its business fraud claim under Section 17200 of the California Business and Professions Code not for the purposes of argumentation but to preserve the issue.

² Citations to "¶" refer to the SAC.

Moreover, a measurable, regular flow of anomalous bot activity on X's platform forces it to purchase an [REDACTED] server load capacity on average as well as the energy necessary to run these servers as a business imperative: this amounts to an additional [REDACTED] [REDACTED]. ¶ 69. In other words, although X rarely suffers distributed denial-of-service attacks that take its services offline altogether, X would regularly suffer such complete server failures if it did not budget server capacity in advance based on the regularized flow of anomalous traffic to its systems. ¶¶ 68-73. And as a social media platform premised on moment-to-moment availability for its users, X all but has to purchase this additional server load. See ¶¶ 18-39, 68-73. X should not be required to sit idly by and wait until scrapers like Bright Data and its customers' degradation and diminishment of X servers wreck those servers altogether—particularly as it seeks both injunctive relief and damages—before obtaining an enforceable right to exclude. As a market-leading purveyor of scraping crawlers specifically targeted at X, ¶¶ 82-100, Bright Data cannot escape the plausible inference that it (by itself or through its customers) contributes on a massive scale to this specific, diminished server capacity.

(a) *Trespass to Chattels*

The scraping burden Bright Data imposes on X's servers is not lighter than nor akin to legitimate user traffic. The Supreme Court of California has held that “trespass to chattels lies where an intentional interference with the possession of personal property has proximately caused injury.” *Intel Corp. v. Hamidi*, 71 P.3d 296, 302 (Cal. 2003) (cleaned up). This Court queried whether the scraping is inherently burdensome at all—even positing that some type of web crawling might be less burdensome than legitimate X user activity. Op. at 9-10. The SAC avers to the contrary: Bright Data's proxy services allow Bright Data and its customers to circumvent the rate limits imposed such that they can query X's servers over and over again, and X's internal estimates are that scraping generally entails about a million times more requests to X servers than a normal user would make. ¶¶ 76-82.

These allegations similarly refute Bright Data's previous argument that it could not be liable for trespass to chattels because X “consented to participate in a worldwide communications network, known as the World Wide Web, when it connected its servers to the internet.” ECF No. 42 at 23.

1 As in *Knight v. Jewett*, 834 P.2d 696, 711 (Cal. 1992), Bright Data’s conduct is “totally outside of the
 2 range of the ordinary activity involved”—that is public surfing of X and its platform. *Id.* Although
 3 X is a semi-public platform, it is not open access because it restricts the amount of content both
 4 logged-in and logged-out users can access; the only way to go beyond these rate limits is to
 5 circumvent X’s technological measures. ¶¶ 55-67.

6 In other words, the only possible way to reach such a scale requires far exceeding ordinary
 7 human internet browsing. ¶¶ 59, 67, 87, 89-92. The court in *eBay, Inc. v. Bidder’s Edge, Inc.* made
 8 this precise observation when it noted that “even if [defendant]’s web crawlers were authorized to
 9 make individual queries of [plaintiff’s] system, [defendant’s] web crawlers exceeded the scope of any
 10 such consent when they began acting like robots by making repeated queries.” 100 F. Supp. 2d 1058,
 11 1070 (N.D. Cal. 2000). Just so here: X has not consented to—and indeed repeatedly warned users
 12 via its Terms that it does not consent to—automated, mass usage. *See* ¶¶ 28-31, 76-82. This is not a
 13 new innovation in the law. California’s trespass to chattel doctrine has long recognized that property-
 14 holders may offer limited consent to access, and liability falls on a party who “proceeds to exceed
 15 those limits by divergent conduct.” *Civic Western Corp v. Zila Industries, Inc.*, 135 Cal. Rptr. 915,
 16 925 (Cal. Ct. App. 1977). Put simply, although X may have consented to Bright Data and its
 17 customers using X’s platform in some capacity, it did not authorize or give its consent to its mass-
 18 scale usage necessary for it to sell vast quantities of scraped X data. With the addition of the above-
 19 discussed allegations in the SAC which quantify the harm flowing to X from Bright Data’s
 20 unauthorized access, ¶¶ 68-75, X’s trespass to chattels claim can stand.

21 **(b) Tortious Interference with Contract**

22 The Court already found X sufficiently alleged the existence of valid, enforceable third-party
 23 contracts as to which Bright Data induced breach. Op. at 14. (citing *Pac. Gas & Elec. Co. v. Bear*
 24 *Stearns & Co.*, 791 P.2d 587, 589–90 (Cal. 1990) (“The elements of a tortious interference with
 25 contractual relations claim are (1) a valid contract between plaintiff and a third party, (2) defendant’s
 26 knowledge of this contract, (3) defendant’s intentional acts designed to induce breach or disruption
 27 of the contractual relationship, (4) actual breach or disruption of the contractual relationship, and (5)
 28 resulting damage.”). With X’s measurable allegations of damages to its systems flowing directly

1 from Bright Data’s customers’ automated access to X’s servers, ¶¶ 68-75, X’s tortious interference
 2 with contract claim is ripe to proceed so that X can unmask those who Bright Data has induced to
 3 abuse X’s system access.

4 (c) *Breach of Contract*

5 After reciting the familiar breach of contract elements, the Court also found that “even
 6 assuming Bright Data shut down its registered account(s) and that this had the effect of terminating
 7 its click-wrap contract(s) with X Corp., there is no question that Bright Data remained bound by the
 8 Terms [restricting accessing or scraping X’s platform], having impliedly agreed to them in ongoing
 9 scraping.” Op. at 15-17 (citing *Oasis W. Realty, LLC v. Goldman*, 250 P.3d 1115, 1121 (Cal. 2011)
 10 (“The elements of a breach-of-contract claim are (1) the existence of a contract, (2) plaintiff’s
 11 performance or excuse for nonperformance, (3) defendant’s breach, and (4) resulting damage.”)). The
 12 SAC now details the particular ways by which Bright Data’s breaching conduct results in damages:
 13 specifically, increased server, energy, operational, and maintenance costs. ¶¶ 68-75. X thus states a
 14 plausible breach of contract claim based on Bright Data’s automated access of X’s servers.

15 2. Amended Data Scraping Claims Are Not Preempted

16 Although federal law is granted supremacy over state law under the Constitution, there is a
 17 presumption that “the historic police powers of the States were not superseded by [federal law] unless
 18 that was the clear and manifest purpose of Congress.” *Wyeth v. Levine*, 555 U.S. 555, 565 (2009).
 19 Federal law does not preempt historically grounded state causes of action when their purpose is to
 20 vindicate “a substantial state law interest, i.e., an ‘interest[] outside the sphere of congressional
 21 concern in the [copyright] laws,’ that is ‘distinct from the interests served by the federal law which
 22 may preempt the claim[s].’” Op. at 25; *In re Jackson*, 972 F.3d 25, 37 (2d. Cir. 2020) (quoting *Bonito*
 23 *Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 155 (1989)) (alterations in original). The
 24 Court correctly noted that privacy is just such an interest because “the protection of privacy is not a
 25 function of the copyright law,” *Garcia v. Google, Inc.*, 786 F.3d 733, 745 (9th Cir. 2015), but stated
 26 that “X Corp.[] is not looking to protect X users’ privacy.” Op. at 25. In fact, however, as the SAC
 27 details, protection of privacy as well as several additional substantial state law interests do support
 28

1 X's breach of contract and tortious interference with contract claims based on damages flowing from
2 scraping.

3 (a) *Preventing Bright Data's Scraping Will Protect X Users' Privacy*

4 X is a business that, among other things, aggregates, packages, and sells X user content, **but**
5 ***it does so with express limits, to protect X user privacy.*** As the SAC explains, these limits include
6 the ability for X users to tailor their privacy settings and adjust those settings over time such that
7 developers with access to X's API subscription service are required to delete the data which X users
8 no longer wish to be public. ¶ 75. If an X user (or X) protects, modifies, deletes, or blocks content,
9 X developers must do the same with that content. ¶¶ 35-38, 44, 47(a)-(d). For example, X removes
10 revenge porn or the sharing of personally identifiable information like social security numbers. ¶¶
11 47, 51(b). X does not sell all data which is publicly available on the X platform. *See* ¶ 44, 47(g). For
12 the types of data it does sell, it places restrictions on what X user data it offers for sale to developers
13 through this API subscription access: X developers cannot use X data to infer X user protected
14 characteristics, even if an X user publicly posts this information. ¶ 47(g). X developers may not use
15 acquired data for tracking or targeting sensitive groups, such as political activists or dissidents. ¶
16 47(j). To obtain the highest Enterprise subscription tier, developers must affirmatively apply for
17 approval of the use case for which they seek to X enterprise-level data access. ¶ 42. X places similar
18 restrictions on its own internal uses of its data to sell targeted advertisements to its users. ¶¶ 48-49.
19 Finally, "if X registered users grow dissatisfied with X's particular cocktail of public-private content-
20 and-data sharing, X users can delete their registered X accounts such that X and its developers
21 eventually delete that content and data as well." ¶ 75. The substantial state privacy interest that X
22 users maintain limited control over is therefore similar to the right of publicity: these claims are not
23 preempted by the copyright laws because although someone's likeness is in the public domain, he or
24 she maintains the "prerogative not to have his or her name, likeness, voice, or identity used in a
25 commercial advertisement, whether that citizen is a celebrity or not." *Facenda v. N.F.L. Films, Inc.*,
26 542 F.3d 1007, 1032 (3d Cir. 2008) (emphasis in original).

27 Bright Data does not offer analogous privacy protections. Bright Data places almost no
28 restrictions on the use of data scraped from X. ¶¶ 107-109. Bright Data does not prohibit itself (or

its customers) from identifying X users based on the characteristics which X protects, or tracking them based on the same. ¶¶ 109(a)-(d). Bright Data does not prohibit matching X usernames to legal identities or personally identifying information. ¶ 109(c). Bright Data does not prohibit using X user’s geodata to track them, or make heatmaps. ¶ 109(d). Perhaps most importantly, Bright Data and its customers also need not delete or modify any content when it is deleted or modified on X—for example, revenge porn or improperly shared social security numbers. ¶ X 109(a).

Even if Bright Data offered privacy options anywhere near as compelling as those X offers its users, one of Bright Data’s express selling points is that it offers its customers “total anonymity.” ¶¶ 102-06. Once Bright Data or its customers scrape X user data, those X users have no way of learning that some other actor possesses that data aggregated in the ether. ¶¶ 105-06. There are thus almost no circumstances under which X users can claw this data back. *See* ¶¶ 107-09. The privacy gap between X and Bright Data is thus particularly wide: X users have a measure of control over their data on X but almost none, if any, with scrapers like Bright Data. *See* Note, Geoffrey Xiao, *Bad Bots: Regulating the Scraping of Public Personal Information*, 34 HARV. J. L. & TECH. 702, 711 (2021). While Bright Data might note it is subject to the CCPA or the GDPR, Bright Data still is not registered as a “data broker” under California law despite ostensibly qualifying as one.³ ¶ 107.

In other words, scrapers like Bright Data break the consent structure on which users rely for limited control over their privacy connected to the platforms they use, including X. ¶¶ 22-50, 75, 95, 102, 103-106, 109. At bottom, X users know to whom to turn (or whom to ask what to delete) when they have an issue with their privacy on the X platform: X. ¶¶ 35-39; *see also Stackla, Inc. v. Facebook Inc.*, No. 19-cv-05849 PJH, 2019 WL 4738288, at *6 (N.D. Cal. Sept. 27, 2019) (“Facebook’s ability to decisively police the integrity of its platforms is without question a pressing public interest.”). No wonder governmental representatives from foreign countries such as Australia, Canada, the United Kingdom, Switzerland, Norway, New Zealand, Colombia, Morocco, Argentina, and Mexico recently issued a “Joint statement on data scraping and the protection of privacy” that

³ A “data broker” is defined as a “business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.” ¶ 107 n.8.

1 highlights the risks to privacy flowing from inadequate prevention of scraping by social media
 2 platforms such as X.⁴ ¶ 108. As X is the source of X user data at scale, it is most efficient for the
 3 onus to be on X to regulate access to X's data (or for countries such as those mentioned above to
 4 regulate user data and privacy by regulating X). ¶¶ 75, 108. In short, X users enjoy a limited measure
 5 of privacy when entrusting X with their data, but this privacy interest is destroyed if Bright Data can
 6 scrape with impunity: anything anyone posts publicly on any platform could be preserved *forever*, no
 7 matter how quickly that person thinks better of what they shared and deletes it. And that data may be
 8 used and sold, not in the privacy-preserving ways as X requires, but by and to anyone and for any
 9 purpose. *See* ¶¶ 93-109.

10 (b) *Election Integrity and Public Conversation Manipulation*

11 X also makes significant efforts to stop foreign interference or improper manipulation of
 12 public conversations on matters of public concern, often to protect the sanctity of elections and the
 13 democratic process. *See* ¶¶ 43, 50-54; *see also* Mekela Panditharatne, *Preparing to Fight AI-*
 14 *Backed Voter Suppression*, BRENNAN CTR. FOR JUSTICE (Apr. 16, 2024), available at
 15 [https://www.brennancenter.org/our-work/research-reports/preparing-fight-ai-backed-voter-](https://www.brennancenter.org/our-work/research-reports/preparing-fight-ai-backed-voter-suppression)
 16 [suppression](https://www.brennancenter.org/our-work/research-reports/preparing-fight-ai-backed-voter-suppression). To that end, X has blacklisted developers with IP addresses originating from certain
 17 high risk jurisdictions from purchasing its API data access. ¶ 43. Bright Data does not impose
 18 similar restrictions, and other scrapers need not as well. ¶ 109. While Bright Data styles itself as a
 19 white knight of the open internet, its proxy servers enable bad actors – from where, who knows?
 20 Certainly neither X nor its users. This anonymity, which Bright Data advertises and enables, ¶ 95,
 21 103-06, allows its customers to cloak bad intentions and build up data for potentially nefarious ends.

22 As for X, in February 2021 X disclosed it removed 373 accounts and related content
 23 attributed to state-linked information operations originating from Iran, Armenia, and Russia. ¶ 52.
 24 X disclosed in December 2021 that it removed 3,465 accounts connected to state-linked information
 25 operations from eight other jurisdictions: Mexico, the People's Republic of China (PRC), Russia,
 26

27 ⁴ Glob. Priv. Assembly, Int'l Enf't Coop. Working Grp., *Joint Statement on Data Scraping and the*
 28 *Protection of Privacy* (Aug. 24, 2023), <https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf>.

1 Tanzania, Uganda, and Venezuela. Every account and piece of content associated with these
 2 operations was permanently removed from the X platform.” *Id.* If X and other similar social semi-
 3 public social media platforms are defenseless to stop scraping, there is little, if anything, standing in
 4 the way of foreign governments (including those hostile to the United States) and other nefarious
 5 actors hoovering up terabytes of data on every American who uses platforms such as X.

6 (c) *X and Consumer Protection*

7 X’s state law claims further advance the substantial state interest of consumer protection.
 8 Courts often invoke consumer protection to reject assertions of federal preemption, including in
 9 actions instituted by self-interested private parties. *See, e.g., In re JUUL Labs, Inc., Mktg., Sales*
 10 *Pracs., & Prod. Liab. Litig.*, 497 F. Supp. 3d 552, 592-93 (N.D. Cal. 2020) (declining to hold that
 11 the FDA’s regulations preclude product liability claims); *Jackson*, 972 F.3d at 37-38 (“preventing
 12 consumer deception” is substantial state interest). Other courts have held that “[b]ecause consumer
 13 protection law is a field traditionally regulated by the states, compelling evidence of an intention to
 14 preempt is required in this area.” *General Motor Corps v. Abrams*, 897 F.2d 34, 41-42 (2d Cir.
 15 1990).

16 Here, X has a number of contractual rules and policies meant to protect its users and the market
 17 from manipulation that would be undermined if Bright Data can scrape X’s data at scale to manipulate
 18 or defraud the market—for example, to generate baseless interest in or gauge the optimal moment to
 19 cash in on cryptocurrency scams. ¶¶ 50-51, 53-54. Indeed, the Ninth Circuit has already
 20 acknowledged in another context that the “dangers of social media, in its current form, are palpable”
 21 due to the potential presence of false and misleading information. *Gonzalez v. Google LLC*, 2 F.4th
 22 871, 950 (9th Cir. 2021) (Gould, C.J., concurring and dissenting in part), rev’d sub nom. on other
 23 grounds, *Twitter, Inc. v. Taamneh*, 598 U.S. 471 (2023). In the adjacent context of product liability
 24 law, the Supreme Court has held that preemption is rarely warranted where “history emphasizes the
 25 importance of providing an incentive to businesses to use the utmost care in the business of
 26 distributing inherently dangerous items.” *Bates v. Dow Agrosciences LLC*, 544 U.S. 431, 449-50
 27 (2005) (discussing the need to limit preemption in suits against chemical manufacturers). Allowing
 28 just anyone to access X user data at scale dampens the incentives and tools available for X to optimally

1 police its platform against potential manipulation: if X knows who is accessing its own API data
 2 systems *and* can profit from this access, it both has the recourse and the incentive to take the requisite
 3 steps to ensure compliance. Similarly, control over third-party access to X user data is necessary to
 4 limit fraudulent actors’ use of X data, especially given that scraped data is used for phishing and other
 5 acts of consumer deception. ¶¶ 50-54.

6 (d) *Regulating Economic Activity*

7 X’s claims also deliver on the state interest of deterring misbehavior in business
 8 transactions. California courts have, for example, held that the “principle of unjust enrichment . . .
 9 is broader than mere ‘restoration’ of what the plaintiff lost” and instead is focused on “the public
 10 policy of this state[, which] does not permit one to take advantage of his own wrong[,] regardless of
 11 whether the other party suffers actual damage.”⁵ *Cnty. of San Bernardino v. Walsh*, 69 Cal. Rptr. 3d
 12 848, 854-55 (Cal. Ct. App. 2007) (internal quotation marks and citation omitted). Without the
 13 availability of such a cause of action, California courts have held, “there would be an insufficient
 14 deterrent to improper conduct that is more profitable than lawful conduct.” *Id.* at 856. Federal
 15 courts have used that same logic to hold that federal copyright law does not preempt tort claims that
 16 serve the purpose of deterring unscrupulous business practices. For example, in *Digital Drilling*
 17 *Data Systems, LLC v. Petrolink Services, Inc.*, 965 F.3d 365 (5th Cir. 2020), the plaintiff alleged
 18 that the defendant induced its customers to breach their contracts as part of an effort to access
 19 restricted data on the plaintiff’s system. The Fifth Circuit found the claim not preempted, in part
 20 due to the fact that the tort claims embodied a state interest in preventing “the taking of undue
 21 advantage.” *Id.* at 382. X’s misappropriation claim in particular similarly deters bad actors who
 22 “deprive [firms] of their fair share of the benefits of the parties’ common venture.” *See Andrews v.*
 23 *Daughtry*, No. 12-cv-00441, 2013 WL 664564, at *13 (M.D.N.C. Feb. 22, 2013); ¶¶ X-X.
 24 Moreover, California law recognizes a public policy of preserving “contractual stability” in the
 25 economy whereas much of Bright Data’s business model is predicated on inducing breach of
 26

27 ⁵ Beyond finding it preempted, the Court did not address X’s unjust enrichment claim, which it
 28 pled in the alternative. ¶¶ 132-38. X stands on its previous briefing in support of this claim. ECF
 No. 48 at 24-26.

1 contract relative to some of California’s most prominent companies. *See, e.g., I-CA Enterprises,*
 2 *Inc. v. Palram Americas, Inc.*, 185 Cal. Rptr. 3d 24, 50-51 (Cal. App. Ct. 2015).

3 X’s claims also support California’s state interest in ensuring the regulated flourishing of
 4 businesses within a state’s borders. For example, the Supreme Court upheld California’s anti-piracy
 5 laws in 1973, finding the Copyright Act did not preempt them, in part because of the state’s interest
 6 in prohibiting “conduct that may adversely affect the continued production of new recordings, a large
 7 industry in California.” *Goldstein v. California*, 412 U.S. 546, 571 (1973). Especially in California,
 8 the continued viability of internet and technology companies such as X is an important economic state
 9 interest. Similar to “hot news” misappropriation, Bright Data is “free riding on [X’s] efforts,” and
 10 “the ability of other parties to free-ride on the efforts of the plaintiff or others would so reduce the
 11 incentive to produce the product or service that its existence or quality would be substantially
 12 threatened.” *Nat’l Basketball Ass’n v. Motorola, Inc.*, 105 F.3d 841, 845 (2d Cir. 1997). In other
 13 words, California has a substantial state interest in ensuring one of its primary industries continues to
 14 thrive. As the SAC demonstrates, the business models of several of California’s prominent internet
 15 and social media companies, not just X, would be threatened if copyright preemption made it
 16 impermissible to restrict scrapers like Bright Data. ¶¶ 5, 18-54. This is all the more the case because,
 17 as is true here, Bright Data conducts “unauthorized interference with the normal operation of
 18 complainant’s legitimate business precisely at the point where the profit is to be reaped, in order to
 19 divert a material portion of the profit from those who have earned it to those who have not.” *Barclays*
 20 *Capital Inc. v. Theflyonthewall.com, Inc.*, 650 F.3d 876, 877 (2d Cir. 2011) (quoting *Int’l News Serv.*
 21 *v. Associated Press*, 248 U.S. 215, 240 (1918)).

22 3. Misappropriation of X’s Aggregated Data At Scale

23 Assuming X’s misappropriation claim is not preempted, California common law
 24 misappropriation claims require that 1) the plaintiff made a substantial investment of time, effort, and
 25 money into creating the thing misappropriated such that the court can characterize the ‘thing’ as a
 26 kind of property right; (2) the defendant appropriated the ‘thing’ at little or no cost; and (3) the
 27 defendant injured the plaintiff by the misappropriation. *Hollywood Screentest of Am., Inc. v. NBC*
 28 *Universal, Inc.*, 151 Cal. App. 4th 631, 650 (2007). X’s misappropriation claim survives for all the

1 reasons previously enumerated, ECF No. 48 at 28-30, and for the additional reason that it is alleging
2 a property interest in the resource it created: aggregated X data at scale. ¶¶ 153-58.

3 Aggregated data at scale is a qualitatively different resource than individual X “user content.”
4 Cf. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012),
5 <https://repository.law.umich.edu/mlr/vol111/iss3/1> (exploring “mosaic theory” that technology-
6 enabled large scale data collection over time creates a qualitatively different data type than individual
7 or small scale data points in Fourth Amendment privacy context). It is aggregated data at scale, not
8 individual public “user content,” to which X seeks to exclude access. ¶¶ 55-67. One major purpose
9 of X’s platform is to give its users the option to freely make individual user content available to public
10 *for its human users*: the use case for X’s user-side platform is specifically to serve as a public forum
11 for public conversations. ¶¶ 18-39. It is not possible, though, for an individual human to package
12 data at the velocity and volume necessary to convert it into aggregated data at scale. See ¶¶ 87-92.
13 Thus, X does not seek to restrict Bright Data’s access to public information or X users’ licensed
14 content, as Bright Data asserts, ECF No. 49 at 20-23. X is instead restricting the right to scrape and
15 exploit the resource it has created by offering its user-side platform to the public at zero cost.

16 The Eleventh Circuit has addressed the intersection of data scraping and aggregated data at
17 scale in the trade secret misappropriation context. *Compulife Software Inc. v. Newman*, 959 F.3d
18 1288 (11th Cir. 2020). There, Compulife, a company that produced a database of life insurance
19 quotes, sued a competitor for, *inter alia*, misappropriating trade secrets. *Id.* at 1313-15. While
20 Compulife’s database was publicly available, individual users were only able to retrieve individual
21 quotes from the database. *Id.* Under this structure, the Eleventh Circuit observed that it would take
22 too long for a single person to retrieve every quote in the database. Thus, in some sense the public
23 did not have access to the entire database; the public had access only to individual requested quotes.
24 *Id.* Even though the database aggregated at scale was technically available to the public, it could not
25 practically be recreated or copied in its entirety by any single person. *Id.* Similar to the scraping at
26 issue here, the defendant there used a data scraping bot to request an impossibly large number of
27 quotes from Compulife’s database—40 million quotes. The Eleventh Circuit reasoned that
28 “[a]lthough Compulife has plainly given the world implicit permission to access as many quotes as is

1 humanly possible, a robot can collect more quotes than any human practicably could.” *Id.* at 1314.
 2 “So,” the Eleventh Circuit went on, “while manually accessing quotes from Compulife’s database is
 3 unlikely ever to constitute improper means [for trade secret misappropriation analysis], using a bot to
 4 collect an otherwise infeasible amount of data may well be.” *Id.* The Eleventh Circuit even observed
 5 that Compulife’s failure to put a use restriction on its website did not automatically render that data
 6 *as a whole* publicly available. By contrast, here, X did impose an express use restriction in its Terms,
 7 making its claims *even stronger* than those sustained by the Eleventh Circuit in *Compulife*. ¶ 22.

8 Based on this reasoning, the Eleventh Circuit concluded that a data scraper might
 9 misappropriate trade secrets by copying an entire database, even when individual data points from
 10 that database were technically available to the public. *Id.* at 1315. Similarly, X asserts a protectable
 11 property interest in the synergistic combination of the parts it cultivated through building its multi-
 12 sided platform. ¶¶ 153-58. If Bright Data can continue to free-ride on X’s aggregated data at scale,
 13 X will likely continue to experience a spiral of negative indirect network effects. *C.f. Ohio v. Am.*
 14 *Express Co.*, 585 U.S. 529, 544 (2018) (noting multi-sided markets face risk of indirect network
 15 effects from one side of the market leading to feedback loops on the other sides). X has already
 16 *voluntarily* degraded X’s unregistered user experience by throttling public access to X content in an
 17 attempt to stop scrapers like Bright Data. ¶¶ 55-65. If Bright Data’s misappropriation of X’s
 18 aggregated data at scale is legally sanctioned, X and other social media platforms that offer free user
 19 access may eventually have to rethink their business models altogether. *See* ¶¶ 18-54. Courts have
 20 recognized these ills are not hypothetical chimeras in similar contexts. *See e.g., Facebook, Inc. v.*
 21 *ConnectU LLC*, 489 F. Supp. 2d 1087, 1091-93 (N.D. Cal. 2007) (sustaining social media company’s
 22 misappropriation claim based on scraping of its user email data and further finding no copyright
 23 preemption). This Court should follow.

24 **B. X’s Amendments Are Timely And Do Not Prejudice Bright Data**

25 *First*, X’s amendments do not prejudice Bright Data. The party opposing the amendment
 26 bears the burden of showing prejudice. *Eminence Cap.*, 316 F.3d at 1052. Where the defendant is
 27 on notice that the claims existed and where the proposed amendment does not represent any “major
 28 change in the scope of the claims or in the tenor of the case” there is no prejudice. *Johnson v. Serenity*

1 *Transportation, Inc.*, No. 15-cv-02004-JSC, 2015 WL 4913266, at *5 (N.D. Cal. Aug. 17, 2015)
2 (finding no prejudice and granting leave to amend). Here, X is not adding new claims to the case (it
3 is even dropping one); X added only allegations necessary to address the Court’s identified
4 deficiencies. Moreover, this dispute is in its incipiency: X has amended its complaint only once, and
5 the case has not commenced with meaningful discovery on the merits. Bright Data cannot, therefore,
6 show any cognizable prejudice flowing from granting X leave to amend.

7 *Second*, there has been no undue delay. X filed this motion for leave to amend by the Court’s
8 June 6 noon deadline. Op. at 26. And there is not yet an operative deadline for amendments to
9 pleadings. *See* ECF No. 55.

10 *Third*, this is X’s first motion to amend its complaint. X previously amended as a matter of
11 right, and those amendments undoubtedly contributed to the Court finding it could exercise personal
12 jurisdiction over Bright Data. ECF No. 67. As such, there has been no “repeated failure” to cure
13 deficiencies. *Eminence*, 316 F.3d at 1052.

14 **V. CONCLUSION**

15 For the foregoing reasons, X respectfully requests that the Court grant X’s motion for leave
16 to file the SAC.

1 DATED: June 6, 2024

Respectfully submitted,

2 QUINN EMANUEL URQUHART &
3 SULLIVAN, LLP

4 By /s/ Andrew H. Schapiro

5 Andrew H. Schapiro (*Pro Hac Vice*)
andrewschapiro@quinnemanuel.com
6 191 N. Wacker Drive, Suite 2700
Chicago, IL 60606-1881
7 Telephone: (312) 705-7400

8 David Eiseman (Bar No. 114758)
davideiseman@quinnemanuel.com
9 50 California Street, 22nd Floor
San Francisco, California 94111-4788
10 Telephone: 415-875-6600
Fax: 415-875-6700

11 Stefan Berthelsen (*Pro Hac Vice*)
stefanberthelsen@quinnemanuel.com
12 51 Madison Ave 22nd floor
13 New York, NY 10010
14 Telephone: (212) 849-7014

15 *Attorneys for Plaintiff X Corp.*